REMARKS

Applicant has filed the present Amendment and Response in reply to the outstanding Official Action of February 10, 2006, and Applicant believes the Amendment and Response to be fully responsive to the Official Action for the reasons set forth below in greater detail.

At the onset, Applicant would like to note that Claims 1 and 7 have been amended herewith. Specifically, the claims have been amended to correct several minor editorial errors. Claims 1 and 7 are amended to delete the phrase "as well as". The claims were also amended to provide proper antecedent basis for "appropriate work computer" and for "the programs required". Applicant submits that the amendments overcome the first three 35 U.S.C. § 112, second paragraph rejections.

Applicant respectfully disagrees with the Examiner's last § 112 rejection and traverses based at least upon the following analysis. There is sufficient antecedent basis for the registering part and central processing part. Each computer, e.g., first work computer and second work computer include a registering part and a processing part. These parts are distinctly claimed as separate elements and limitations. Similarly, the server computer includes at least a registration part for registering personal verification information. The server computer is also separately claimed. Therefore, each distinct limitation should have a separate reference to a registering part and a processing part, etc.

In the Official Action, Claims 1-10 stand rejected under 35 U.S.C. § 102(e) as being anticipated by Tran, United States Patent No. 6,505,238. Tran is a newly cited

reference. Applicant respectfully disagrees with the rejection and traverses with at least the following analysis.

The reference does not teach, "an **attachable mobile media** for housing encrypted personal verification information **and the programs required for operating that work computer**", as recited in Claim 1. Additionally, Applicant submits that the reference fails to teach that personal verification information is sent from said first work computer via said server computer to said second work computer, which is also recited in Claim 1.

The reference teaches that program information is stored in a server. The client terminal or local server acts as a server to the remote search terminal. Tran describes that the "computer networks are made accessible to a remote client via the Internet by **storing the necessary software on the network servers and client terminals**. The software further permits a client terminal to be simulated on the remote search terminal of a user who has entered the proper credential information." Col. 6:60-65. The described system uses a Lightweight directory Access Protocol (LDAP) technology. On the global network, a client computer and local server are categorized into sub-groups. The invention contemplates structuring every organization in the world in a similar manner. Organizations that are networked will then allow LDAP to conduct hierarchical **searches for a particular location and user client terminal**. The invention is designed to allow a user to remotely access a client terminal's settings via a website.

The method is described as follows:

> 1.) Using a Web Browser, the user enters the organization's URL. This opens the login web page of the organization stored in the memory of the network server; (2.) From this **web**

> **page**, the user is permitted to login to his workstation by entering the proper credential information including his user id and password; and (3.) Once the user provides the correct credential information, the **network applications and personal applications, data, email, etc. are simulated, on and fully accessible from the remote search terminal as if the user were using his own workstation**.

This system is equivalent to a virtual office system.

In the preferred embodiment, the reference describes that both the encrypted personal verification information and the programs required for operating that work computer are not stored on an attachable media, rather stored on an local network or client computer. In the preferred embodiment, the **credential data is kept in the local server** where the user's network is located and not in the central database of the organization in order to avoid excess overhead of the organizations central server. Col. 8, lines 46-50. Also, the user's client terminal is automatically simulated by the described invention, **without even mentioning an attachable media** (in the preferred embodiment). Selecting the net search button 414 then automatically simulates the user's client terminal. Col. 11, lines 16-18.

In an alternate embodiment, the specification describes that a smart card can be used where the sub-group name is stored on the card so that the user does not need to enter the login information, just a pin. The specification describes:

> It is important to note that while the present invention has been described in the context of a fully functional data processing system, those skilled in the art will appreciate that the mechanism of the present invention is capable of being distributed in the form of a computer readable medium of instructions in a variety of forms, and that the present invention applies equally, regardless of the particular type of signal bearing media utilized to actually carry out the distribution. Examples of computer readable

> media include: nonvolatile, hard-coded type media such as Read Only Memories (ROMs) or Erasable, Electrically Programmable Read Only Memories (EEPROMs), recordable type media such as floppy disks, hard disk drives and CD-ROMs, and transmission type media such as digital and analog communication links.

Col. 12, lines 13-27.

At best, the reference teaches that the card can be used to access the personal settings from the network, i.e., client server or local server. However, this is not a teaching that this information is housed within the mobile media.

Accordingly, the reference fails to teach that the first work computer provides an attachable mobile media for housing encrypted personal verification information **and the programs required for operating that work computer.**

While it appears that the function of Tran is similar, i.e., to provide the same computer environment, the structure or means for performing the function is different. In contrast, the claimed invention provides the same computing environment in a location different to the location of the original computing environment **through a mobile media carried by a user**, which houses **programs** that are set for a computer environment of that individual user.

The mobile media is inserted into the second workstation and the second workstation operates with the first computing environment. The mobile media can be attached to a work computer, and when a user moves, that user can carry mobile media to the destination work computer where mobile media is used as it is attached thereto. A second work computer is set to be booted up from **an attached mobile media**.

Furthermore, personal verification information **is not sent from said first work computer via said server computer to said second work computer** in Tran.

None of the described embodiments teach or suggest that the personal verification information is sent from **the first work computer**. For example, in the preferred embodiment, the credential data is **kept in the local server** where the user's network is located and not in the central database of the organization in order to avoid excess overhead of the organizations' central server. Col. 8, lines 46-50. The local server is not the first work computer. In the alternate embodiment, Smart Card Technology is used where the sub-group's DN name is stored on the card so that the user does not need to enter the login information. However, in this embodiment, a PIN is required to identify his/her authority for using the card.

Accordingly, none of the embodiments teach, suggest or render obvious the claimed features.

Therefore, Applicant submits that Claim 1 is patentably distinct from the cited reference.

With respect to Claim 2, the reference fails to teach "wherein said server computer provides a database for storage of registered information comprised of the **locations** in which said one or multiple second work computers that are registered are **placed and the times they are available for use**". In the Official Action, the Examiner identifies Col. 9, lines 10-40 for support of the rejection. The identified section in no way teaches or suggests the claimed limitation. It appears that the Examiner is misinterpreting the term "search request" described in Tran. The search request described in Tran is a search for the webpage of the network server. Specifically, Tran describes the search process as follows:

> process begins (step 501) when the user enters a search request on the web browser (step 503). LDAP initiates the search of its database to find the web page of the network server (step 505). A check is made to determine if the search request included the user id and password (step 507). If the search request included the user id and password and LDAP is successful in locating the web page, LDAP initiates an automatic login to the user's client terminal (step 508). The client terminal is then simulated on the web browser (step 509).

Col. 9, lines 11-20.

This search is not the same or equivalent to the claimed **locations** in which said one or multiple second work computers that are registered are **placed and the times they are available for use.** The claimed locations are for the second work computers and not the network server. The locations of the second work computers are access points for the user to insert the mobile media or attachable media. Furthermore, there is no suggestion or teaching of a database that includes information regarding the times that the second work computers are available. In fact, the reference does not even mention availability based upon time.

With respect to Claim 3, the reference fails to teach that the server computer accepts reservations for the use of said second work computer only in respect of registered members who have paid membership fees in advance. The reference does not even mention a paid membership fee for use of the remote access system. The reference only teaches that access is limited to users that have credentials. There is no mention of a paid membership. The credentials are used for security purposes only, not to generate a membership fee.

In stark contrast, the claim recites that usage of the second work computer is limited to registered members who **have paid membership fees in advance.** In a

disclosed embodiment, the specification describes that the mobile computing service company forms a contract with the service company providing work computer 3, registers work computer 3 and constructs a database stored in server computer 4, concerning things like the times and places at which work computer 3 is available for use. The user of work computer 2 accesses a database and looks for the times at which a work computer 3, located at a desired location, is available for use. After confirming that a work computer 3 is available for use at a desired time, the user of work computer 2 reserves a time to use that work computer 3. Based on this reservation for use, server computer 4 encrypts the reservation information and sends it to work computer 2. The reservation is stored. The reference fails to teach this reservation process.

With respect to Claim 4, the reference fails to teach that the first, second and server computers have means for encryption/decryption of the same format, encrypt. personal verification information and **reservation information forwarded**, and decrypt information received.

With respect to Claim 8, the reference fails to teach that the second workstation computer comprises two work computers, as specifically recited.

The section identified by the Examiner does not support the rejection. Figure 2 illustrates the access system. The second work computer appears to be the search computer 202. The client computers are equivalent to the first work computer. As illustrated in Figure 2, there is only one search computer 202. Even if the client computers 208 are the second work computer, the client computers are not connected or used as claimed. Therefore, Tran does not teach, suggest or render obvious this limitation.

With respect to Claim 9, the reference fails to teach "a second work computer that **deletes** the personal verification information from a storage part at the point at which the work processes of the appropriate second work computer finish and **delivers information about usage like the usage commencement and completion times to the server computer and wherein the server computer calculates the usage based on the information about usage thus received," as specifically claimed.** Once again, the section identified by the Examiner does not support the rejection. The identified section Col. 11, lines 20-67 references security issues and credentials. There is not even an implication of calculating the usage based on the information thus received. Tran does not even disclose that the system keeps track of usage time. Tran appears to be more concerned with authenticating and security issue. Additionally, the reference does not teach that the second work computer deletes the personal verification information when the user is finished, as claimed.

In a disclosed embodiment, the specification describes that after the user has completed usage of the work computer, the work computer deletes the stored personal verification information for that user from the storage part, encrypts information about the usage, such as when the user started and finished using the work computer, i.e., the usage time, and sends that information to a server computer. The server computer calculates the usage charges based on this usage information. The mobile computing service company collects usage fees from the user based on the usage fees as calculated for the prescribed period. This is a tool whereby the computer service company can calculate a fee to charge its members. The reference is not concerned with access fees.

With respect to Claim 10, the reference fails to teach wherein said server computer **posts notice concerning things like the location of said second computer** and **processes collection of notice fees** from a service company providing said second work computer.

Accordingly, Claims 2-4 and 8-10 are patentably distinct from the cited reference based at least upon the analysis set forth above individually and in view of their dependency, whether directly or indirectly, from independent Claim 1.

Claims 5-7 are patentably distinct from the cited reference based at least upon the analysis set forth above with respect to independent Claim 1.

For all the foregoing reasons, the Applicant respectfully requests that the Examiner withdraw the rejections of Claims 1-10 pursuant to 35 U.S.C. § 102(e). Additionally, Applicant respectfully requests that the Examiner withdrawn the rejections of Claims 1 and 7 pursuant to 35 U.S.C. § 112, second paragraph.

In conclusion, the Applicant believes that the above-identified application is in condition for allowance and henceforth respectfully solicits the Examiner to allow the application. If the Examiner believes a telephone conference might expedite the

allowance of this application, the Applicant respectfully requests that the Examiner call the undersigned, Applicant's attorney, at the following telephone number: (516) 742-4343.

Respectfully submitted,

Seth Weinfeld
Registration No. 50,929

SCULLY, SCOTT, MURPHY & PRESSER, P.C.
400 Garden City Plaza, Suite 300
Garden City, New York 11530
516-742-4343

SW:ae